WILLIAM FRY

// PRIVACY SOURCE

The Role of Data Protection Officers

Amongst the many significant impacts brought about by the new EU General Data Protection Regulation (GDPR), one of the key changes is the introduction of a new role: the mandatory Data Protection Officer (DPO).

The DPO under GDPR

The DPO is now a defined statutory role reporting to the organisation's highest level of management. The DPO is tasked with ensuring an organisation and its employees comply with obligations under GDPR and other relevant legislation, guidance and policies. To ensure organisations comply with the requirement to appoint a DPO, and other requirements of the GDPR, large administrative fines can be imposed for non-compliance.

Appointment of a DPO

The GDPR provides that a DPO must be appointed by an organisation where:

- It is a public body. GDPR further provides that a DPO can be appointed to the role for several public bodies after taking into account the size and organisational structure of the public bodies concerned.
- The organisation's core activities consist of processing operations which by virtue of their nature, scope and/or purposes require regular and systematic monitoring of data subjects on a large scale.
- The organisation's core activities consist of processing special categories of data or data relating to criminal convictions and offences on a large scale. This relates to organisations who store and gather data about the ethnicity, sexuality or health of individuals and organisations who are required to subject staff to Garda vetting or request information about prior criminal convictions.

When considering whether an activity constitutes monitoring, the organisation should consider whether individuals are tracked on the internet. This includes profiling people for the purposes of analysing or predicting personal preferences. This would be applicable to companies who engage in targeted advertising or marketing to individuals and also to companies who monitor individuals through the use of cameras or other means of surveillance.

As the GDPR allows EU member states to add to these categories, the list of organisations in Ireland that are obliged to appoint a DPO may potentially be expanded. Further, even though it may not be required to, there is nothing to prevent an organisation from appointing a DPO for general compliance reasons.

Qualifications

GDPR states that DPOs shall be appointed on the basis of professional qualities, particularly expert knowledge of data protection law and practice. When considering the level of expert knowledge required, the organisation should have regard to the data processing operations carried out and whether specialist expertise may be required. A group think-tank, which the European Commission1[1] took part in, stated that the definition of expert should be interpreted as sufficient knowledge which is possibly a more attainable level of knowledge regarding data protection law and practice.

The Data Protection Commission (DPC) has provided further practical guidance, on their website, on the qualifications required of DPOs to ensure organisations appoint appropriate persons

Position within an organisation

DPOs can either be employees of, or consultants to the appointing organisation. If the DPO is an employee then he or she may still fulfil other tasks or duties provided these other duties do not result in a conflict of interests.

When assessing whether a conflict of interest arises the organisation should be cognisant of whether a DPO may be in a position to offer more favourable treatment to a specific department as a result of his or her position. Due to the potential for a conflict of interest it may be incompatible for the owner of a small business to fulfil the role of DPO as a cost saving measure.

Interestingly the GDPR does not specify that a DPO be a natural person meaning that companies could be appointed as a DPO. Accordingly, a new market has emerged for the provision of DPO services in a manner similar to the provision of company secretarial services.

Role

While the GDPR envisages that the role of a DPO will be a key position within a management structure it also recognises that the appointing organisation must cooperate with and facilitate the DPO in carrying out his or her tasks. Accordingly, the GDPR requires organisations to ensure that the DPO is properly involved in all relevant matters in a timely manner. Independence from the appointing organisation is an important aspect of the DPO role and so an organisation is obliged to ensure that a DPO does not receive any instructions regarding the exercise of his or her tasks.

Furthermore, the GDPR obliges organisations to support the DPO in carrying out his or her tasks by ensuring that the role is properly resourced and an adequate budget is allocated.

Crucially, the GDPR also provides that DPOs cannot be dismissed or penalised by the organisation for performing his or her tasks. We would expect that employment legislation may need to be amended to provide that the dismissal of a DPO for performing his or her role is automatically considered as grounds for an unfair dismissal.

[1] [1] 1 Fablab "GDPR/concepts to operational toolbox, DIY" dated 26 July 2016

Tasks

An important point to note is that DPOs are bound by a statutory duty of confidentiality and secrecy concerning the performance of his or her role. DPOs are prescribed a number of tasks under the GDPR, including:

- Informing the organisation and its employees of their GDPR obligations;
- Monitoring compliance with the GDPR and other applicable data protection rules including the organisation's policies;
- Assigning responsibilities to individuals within the organisation regarding compliance;
- Providing staff training;
- Conducting audits; and
- Acting as the contact point for data subjects who have issues regarding the processing of their data by the organisation and the exercise of their rights under the GDPR.

In addition to these day-to-day tasks, DPOs are also required to cooperate with and act as a contact point for supervisory authorities, i.e. the DPC in Ireland, and to assist the organisation with data protection impact assessments.

The multitude of tasks assigned to a DPO means that organisations that are obliged to implement this role must put significant thought, and resources, into either attracting the right candidate to carry out the role or to assign the duty to an existing resource.

Liability

For organisations, a breach of the requirement to appoint a DPO where one is required could result in the implementation of administrative fines of up to €10,000,000 or 2% of worldwide annual turnover in the preceding financial year, whichever is the higher.

In determining the level of the fine to be imposed for non-compliance with the requirement to appoint a DPO, the DPC must ensure that the fine is proportionate to the infringement. The DPC must also take into consideration, among other factors, the nature, gravity and duration of the infringement, any previous infringements and adherence to approved codes of conduct.

The GDPR does not specifically assign liability to DPOs for a breach of any of his or her obligations such as the duty of secrecy and confidentiality. However, the GDPR requires EU member states to specify rules and other penalties for the breach of GDPR and so DPOs may become subject to penalties and potentially fines for breaches of his or her obligations. No guidance has been issued yet as to how this will operate in Ireland.

Conclusion

A DPO has numerous obligations and a large organisation controlling/processing large amounts of personal data could conceivably require a separate department to ensure compliance with GDPR. It is important to address this requirement immediately if action has not already been taken.

.

Contact Us

If you have any queries in relation to this, or would like to know more about our PrivacySource offering, please contact our Partner below, or your usual William Fry contact.

David Cullen
PARTNER
+353 1 639 5202
david.cullen@williamfry.com

Leo Moore
PARTNER
+353 1 639 5152
leo.moore@williamfry.com

John O'Connor
PARTNER
+353 1 639 51823
john.oconnor@williamfry.com

Contact our PrivacySource Team here

Follow us @WFIDEA